円分体のイデアル類群の構造について ($\mathbb{Z}_p$拡大およびその関連理論の研究)

AUTHOR(S):

館山, 光一

CITATION:

館山, 光一. 円分体のイデアル類群の構造について ($\mathbb{Z}_p$拡大およびその関連理論の研究). 数理解析研究所講究録 1981, 440: 53-63

ISSUE DATE:

1981-10

URL:

http://hdl.handle.net/2433/102818

数理解析研究所講究録
440巻 1981年 53-63

円分体のイデアル類群の構造について

東大　　館山光一

記号

$\mathbb{C}_m = \mathbb{Q}(\exp\frac{2\pi i}{m})$

$\mathbb{C}_m^+ = \mathbb{Q}(\cos\frac{2\pi}{m})$

$C(m)$: $\mathbb{C}_m$ の ideal class group

$C^+(m)$: $\mathbb{C}_m^+$ の ideal class group

j : complex conjugation

$C^-(m) = \{c \in C(m) \mid c^{1+j} = 1\}$

h_m : $\mathbb{C}_m$ の class number

h_m^+ : $\mathbb{C}_m^+$ の class number

$h_m^- = h_m / h_m^+$

E_k : k の unit group

C_K, $C_K^\pm$, h_K, $h_K^\pm$ も同様である。

p を素数とするとき, $C^-(p)$ に関しては, 次の結果が知られている。([1], [2])

$p < 100$, $p \neq 29, 41$ ならば cyclic

$C^-(29) \cong (\mathbb{Z}/5\mathbb{Z})^3$, $C^-(41) \cong (\mathbb{Z}/11\mathbb{Z})^2$

以下これを $(2,2,2)$, $(11,11)$ 型と書くことにする。

また、最近 F. Gerth III ([3]) は $C(68)$ が cyclic であることを特異類の計算によって示した。

ここでは、F. Gerth III, Masley ([4]) の方法を用いて、いくつかの円分体の ideal class group の構造を決定する。

以下体はすべて $\mathbb{Q}$ 上有限次とする。

Lemma 1. K/k : cyclic extension, $G = Gal(K/k)$.

σ : G の generator, $a(K/k) = \#\{c \in C_K \mid c^\sigma = c\}$ とすると

$$a(K/k) = h_k \frac{e(K/k)}{[K:k](E_k : E_k \cap N_{K/k} K^\times)}$$

ここで $e(K/k)$ は k の各素点の分岐指数の積を表す。

Proof) H. Yokoi [5]

次の結果が、Gerth の用いた方法である。

Lemma 2. $[K:k] = 2$, C_K の 2-Sylow sub-group の rank を r, $h_k \not\equiv 0 \bmod 2$ とすると $a(K/k) = 2^r \cdot n$, $(2, n) = 1$

Proof) F. Gerth III [3]

以下ここで用いられる class number に関しては [4], [6], [7], [8] を参照。

Ex 1) $C_{120} = K$ $\quad h_{120} = 2^2$, $\quad h_{60} = 1$

$\Big|$ 簡単な計算より、分岐する素点は2個。

$C_{60} = k$ 故に $a(K/k) = 1 \times \dfrac{2 \times 2}{2 \times (E_k : E_k \cap N_{K/k} K^\times)} \leqq 2$

C_K の rank は1以上であるから $a(K/k) = 2$

よって cyclic。

$C(68)$, $C(168)$, $C(112)$ も同様にできる。

Lemma 3 (Masley's Rank Theorem)

K/k を n 次 cyclic, p を $k \subset E \subsetneq K$ なる任意の中間体に対して $n \mid h_E$ 未0 mod p なる素数とする。このとき C_K の p-rank は f_p の倍数である。ここで f_p は、mod n での p の位数である。

Proof) $c \in C_K$ が order が p であるとする。$\sigma, \tau \in \mathrm{Gal}(K/k)$

$c^\sigma = c^\tau$ とすると、$c = c^{\sigma\tau^{-1}}$。$\sigma\tau^{-1}$ の生成する cyclic group の不変体を F とすると、$\sigma \neq \tau$ ならば、$a(K/F) \equiv 0 \bmod p$, また、lemma 1 より $a(K/F) = h_F \dfrac{e(K/F)}{[K:F](E_F : E_F \cap N_{K/F} K^\times)}$。一方仮定より $h_F e(K/F)$ 未0 mod p。故に $c^\sigma = c^\tau$ ならば $\sigma = \tau$。これより $\#\{c^\sigma \mid \sigma \in \mathrm{Gal}(K/k)\} = n$, C_K の p-rank を r とすると、order p の元は $p^r - 1$ 個あるから、$p^r - 1 \equiv 0 \bmod n$。故に $f_p \mid r$。

Remark) K/k が Galois でも全く同じ命題が成立する。証明も同じである。

Ex 2) $\mathbb{C}_{29} = K$ (Kummer), $h_{29} = 2^3$, $h_k = 1$

$|$

$F(29,4) = k$

ここで $F(29,4)$ は $\mathbb{Q}$ 上拡大次数 4 の $\mathbb{C}_{29}$ の部分体を示す。

$[K : k] = 7$, $2^f \equiv 1 \bmod 7 \Rightarrow f = 3$

(2·2·2) 型となる。

$C(96)$, $C(180)$, $C(41)$ も同様である。

Lemma 4 p を奇素数, K/k を $Gal(K/k) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ なる abelian extension, K_i $(i=1,2,3)$ を K/k の中間体, S_i, S_K をそれぞれ C_{K_i}, C_K の p-Sylow 群とする。このとき

$S_3 = 1$ ならば $S_K \simeq S_1 \times S_2$

Proof) $Gal(K/k) = \{1, \sigma, \tau, \sigma\tau\}$, K_t を $\{1, t\}$ $(t=\sigma,\tau,\sigma\tau)$ の不変体とする。p は奇数より, S_K は 2-uniquely divisible 故に $\varepsilon_t^{\pm} = \frac{1 \pm t}{2}$ とおくと, S_K は次のように分解される。

$$S_K = S_K^{++} \times S_K^{+-} \times S_K^{-+} \times S_K^{--}$$

ここで, 例えば, $S_K^{+-} = \{ c \in S_K \mid c^{\varepsilon_\sigma^+} = c^{\varepsilon_\tau^-} = c \}$ である。

$c \in S_K^{++} \times S_K^{+-}$ とすると $N_{K/K_\sigma}(c) = c^{1+\sigma} = c^{2\varepsilon_\sigma^+} = c^2$, 故に

$N_{K/K_\sigma} : S_K^{++} \times S_K^{+-} \longrightarrow S_{K_\sigma}$ は injective である。

また canonical homomorphism

$S_{K_\sigma} \longrightarrow S_K$

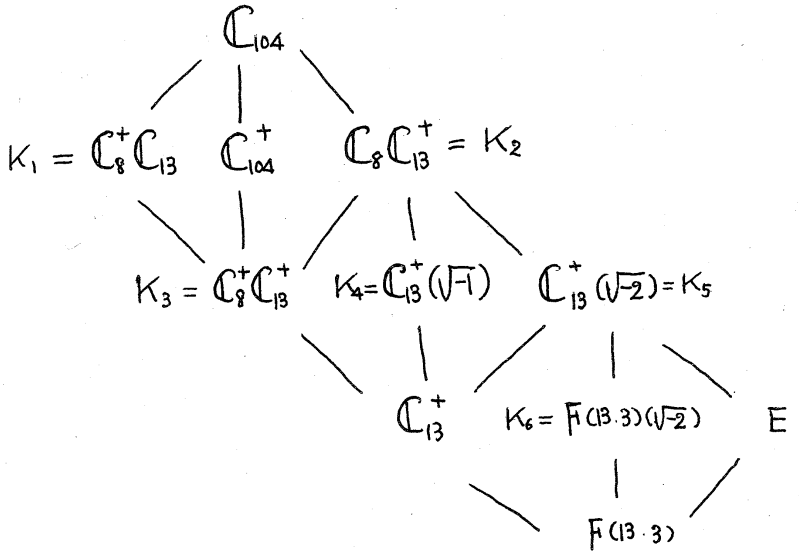
は injective であり，$c \in S_{K\sigma}$ とすると $c^{\xi_\sigma} = c$ より S_K への image は $S_K^{+,+} \times S_K^{+,-}$ に入る。よって $S_{K\sigma} \cong S_K^{+,+} \times S_K^{+,-}$。

同様に $S_{K\tau} \cong S_K^{+,+} \times S_K^{-,+}$，$S_{K\sigma\tau} \cong S_K^{+,+} \times S_K^{-,-}$。

ここで $S_{K\sigma\tau} = 1$ とすると，$S_{K\sigma} \cong S_K^{+,-}$，$S_{K\tau} \cong S_K^{-,+}$

故に $S_K \cong S_{K\sigma} \times S_{K\tau}$ //

Ex 3) $\mathbb{C}_{104}$ $h_{104} = 3^3 \cdot 13$



ここで $F(13\cdot3)$ は，$[\mathbb{C}_{13}^+ : F(13\cdot3)] = 2$ である $\mathbb{C}_{13}^+$ の部分体である。

$h_{K_1} = 3 \cdot 13$ $h_{K_2} = 3^2$, $h_{K_3} = 1$, $h_{K_4} = 3$ $h_{K_5} = 3$

$h_{13}^+ = 1$, $h_{K_6} = 3$.

(3, 3, 3, 13) 型である。

C(144), C(99) は，もっと簡単である。

Lemma 5　p を素数，K/k を p 次 cyclic，$G = \mathrm{Gal}(K/k)$，

S_K, S_k をそれぞれ，C_K, C_k の p-Sylow group であって

次の3つの条件を満たすものとする。

1) $N_{K/k} S_K = S_k$

2) canonical homomorphism $S_k \longrightarrow S_K$ is injective

3) $(S_K : S_k) = p^\lambda$ かつ $\lambda < p-1$

このとき　$S_k = S_K^p$

Proof) 上の仮定より　$S_k \subset S_K$ としてよい。このとき次の様な部分群の列がつくれる。

$S_\lambda = S_k \subset S_{\lambda-1} \subset \cdots \subset S_1 \subset S_0 = S_K$.　　$(S_i : S_{i+1}) = p$

S_i は G-invariant であり，かつ G は S_i/S_{i+1} に trivial に作用する。

σ を G の generator，$c \in S_K$ とすると　$c^{\sigma-1} \in S_1$．帰納的に

$S_i \ni c_i$,　$c = c_0$,　$c_i^{\sigma-1} = c_{i+1}$ とおくと，簡単な計算により

$c^{\sigma^k} = \prod_{i=0}^{k} c_i^{\binom{k}{i}}$,　$c_{p-1} = 1$.　ここで $\binom{k}{i}$ は二項係数を表す。

よって　$N_{K/k} c = \prod_{i=0}^{p-1} c_i^{\alpha_i}$　　$\alpha_i = \sum_{k=i}^{p-1} \binom{k}{i}$　　$\alpha_0 = p$。

$\binom{k}{i}$ は $(1+t)^k$ における t^i の係数であるから，α_i は

$\sum_{k=0}^{p-1} (1+t)^k$ における t^i の係数となる。

$\sum_{k=0}^{p-1} (1+t)^k = \frac{(1+t)^p - 1}{t} \equiv t^{p-1} \mod p$ より　$i \neq p-1$ ならば

$\alpha_i \equiv 0 \mod p$。

また $c_{p-2} = c_{p-3}^{\sigma-1}$ より　$N_{K/k} c_{p-2} = c_{p-2}^p = 1$，さらに帰納法

で $C_i^p = 1$ $(i \neq 0)$ を得る。故に $N_{K/k} C = C^p$ より lemma 5 は証明された。

Ex 4) $\mathbb{C}_{31}$ (Kummer)

$\mathbb{C}_{31}$ $\quad h_{31} = 3^2$, $h_K = 3^2$, $h_k = 3$

$\lambda = 1 < 3 - 1$

$\mathbb{F}(31, 6) = K$ $\quad$ lemma 5 の条件 1) は, K/k が totally ramified であるから, 類体論より成立する。

$\mathbb{Q}(\sqrt{-31}) = k$ $\quad$ 2) は, Kida [10] 参照。($h_{31}^+ = 1$ である)

以上の結果と lemma 5 より $S_k = S_K^3$, 故に S_K は cyclic.

$C(31) \simeq S_K$ より $C(31)$ も cyclic となる。

$C(57)$ も同様に cyclic となる。

Remark) ・$h_m < 10^4$ の場合を考察の対象としたが, 次のような場合は決定できなかった。$C(65)$, $C(156)$, $C(177)$, $C(87)$, $C(240)$。

・$h_m < 10^4$ の場合 $h_m^+ = 1$ が証明されている (Masley [8])。$h_m > 10^4$ の場合 h_m^+ の値がほとんどわかっていない。しかし $C(m)$ ならば, ある程度構造を決定することができる。K, k を imaginary abelian とすると, lemma 1 と同じ記号の下で次の命題が成立する。

Lemma 1′　$a^-(K/k) = \#\{c \in C_K^- \mid c^\sigma = c\}$ とすると

$$a^-(K/k) = h_k^- \frac{e^-(K/k)}{(\mu_k : \mu_k \cap N_{K/k} K^\times)} \cdot 2^\delta \qquad \delta \in \mathbb{Z}$$

ここで $e^-(K/k) = e(K/k)/e(K^+/k^+)$，$\mu_k$ は E_k に含まれる 1 の中根全体のつくる群を表す。

これより，lemma 3 と同様に，次の結果を示すことができる。

Lemma 3′　$p \neq 2$，$nh^- \not\equiv 0 \bmod p$ ならば C_K^- の p-rank は f_p の倍数となる。

lemma 5 は更に単純に，$p \neq 2$，$S_K \longrightarrow S_K^-$，$S_k \longrightarrow S_k^-$ とすればよい。

以上の結果と次の結果を用いることによって，$p \leqq 211$，$p \neq 139, 157$ なる素数 p に対して，$C^-(p)$ の構造を決定することができる。

Lemma 6.　$C_K \supset A$ を次の条件を満たす $\mathrm{Gal}(K/k)$-invariant sub-group とする。$(\#A, [K:k]) = 1$．このとき

$$1 \longrightarrow \mathrm{Ker}\, N_{K/k} \cap A \longrightarrow A \longrightarrow N_{K/k} A \longrightarrow 1 \quad \text{(exact)}$$

は split する。

証明は容易である。

Table I ($h_m < 10^4$)

m	h_m	type	
120	2^2	(2^2)	
29	2^3	$(2,2,2)$	(Kummer)
68	2^3	(2^3)	(Gearth)
31	3^2	(3^2)	(Kummer)
57	3^2	(3^2)	
96	3^2	$(3,3)$	
65	2^6	?	
180	$3\cdot5^2$	$(3,5,5)$	
168	$2^2\cdot3\cdot7$	$(2^2,3,7)$	
41	11^2	$(11,11)$	(Kummer)
156	$2^2\cdot3\cdot13$	?	
104	$3^3\cdot13$	$(3,3,3,13)$	
112	$2^2\cdot3^2\cdot13$	$(2^2,3,3,13)$	
144	$3\cdot13^2$	$(3,13,13)$	
77	$2^8\cdot5$	?	
87	$2^9\cdot3$	?	
99	$3\cdot31^2$	$(3,31,31)$	
240	$2^8\cdot5^2$	$(?,5,5)$	
93	$3^2\cdot5\cdot151$	$(3^2,5,151)$	

Table II $(71 \leqq p \leqq 211)$

p	h_p^- (平方因子でない因子は省略) · type		
71	7^2	(7^2)	(Kummer)
101	5^5	$(5^2, 5^3)$	
113	2^3	$(2, 2, 2)$	
131	$3^3 \cdot 5^2$	$(3, 3, 3, 5^2)$	
137	17^2	(17^2)	
139	$3^2 \cdot 47^2 \cdot 277^2$	$(3^2, ?\ 277, 277)$	
149	3^2	$(3, 3)$	
151	11^2	$(11, 11)$	
157	$13^2 \cdot 157^2$	$(13^2, 157, 157)$	
163	2^2	$(2, 2)$	
197	2^3	$(2, 2, 2)$	
199	3^4	(3^4)	
211	$3^2 \cdot 7^2 \cdot 281^2$	$(3^2, 7^2, 281, 281)$	

Remark) $C(157)$ の 157-Sylow group の構造は,

Iwasawa and Sims, Computation of invariants in the theory of cyclotomic fields,
J. Math. Soc. Japan Vol. 18, No. 1, 1966

で決定されている。

References

1 E. Kummer, Über die Irregularität der Determinaten Monatsber, Akad. d. Wissensh. Berlin, (1853), 194-200

2 K. Iwasawa, A note on ideal class groups. Nagoya Math. J. 27 (1966)

3 F. Gearth, The ideal class groups of two cyclotomic fields. Pro. A.M.S. Vol 78 (1980)

4 J. Masley, Class numbers of real cyclotomic number fields with small conductor. Comp. Math. Vol. 37, (1978)

5 H. Yokoi, On the class number of a relatively cyclic number fields. Nagoya Math. J. 29 (1967) 31-44

6 J. Masley, Solution of small class number problems for cyclotomic fields. Comp. Math. 33 (1976) 179-186

7 G. Schrutka v. Rechtenstamm, Tabelle der (relative-) Klassenzahlen von Kreiskörpern. Abh. Deutsche Akad. Wiss. Berlin 1964 Math. Nat. Kl. Nr. 2.

8 J. Masley, Class groups of abelian number fields Preprint

9 S. Lang, Cyclotomic fields

10 Y. Kida, l-extension of CM-fields and cyclotomic invariant J. Number Theory 12 (1980)